09-27-06

AF

"Express Mail" Mailing Label Number"
EQ667882414US

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE "EXPRESS MAIL POST OFFICE-TO-ADDRESSEE SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED BELOW AND IS ADDRESSED TO COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450 ON:

27 September 2006
DATE OF DEPOSIT

Lisa L. Pringle
SIGNATURE OF PERSON MAILING PAPER OR FEE

Lisa L. Pringle
NAME OF PERSON SIGNING

27 September 2006
DATE OF SIGNATURE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Kenneth Aull
Serial No.	:	09/823,701
Filing Date	:	March 30, 2001
For	:	Preventing ID Spoofing with Ubiquitous Signature Certificates
Group Art Unit	:	2137
Examiner	:	Kevin R. Schubert
Attorney Docket No.	:	NG(MS)7185

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

Sir:

In response to the Notice of Non-Compliant Appeal Brief dated August 28, 2006, please find attached, a revised appeal brief.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Christopher P. Harris
Reg. No. 43,660

TAROLLI, SUNDHEIM, COVELL,
& TUMMINO L.L.P.
1300 East Ninth Street, Suite 1700
Cleveland, Ohio 44114
Phone:(216) 621-2234
Fax: (216) 621-4072
Customer No.: 26,294

I HEREBY CERTIFY THAT ON THE DATE SHOWN BELOW, THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, AS "EXPRESS MAIL POST OFFICE TO ADDRESSEE" MAILING LABEL NO. EQ667882414US

ON 27 SEPTEMBER 2006

SIGNATURE LISA L. PRINGLE

THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Kenneth Aull
Serial No.	:	09/823,701
Filing Date	:	March 30, 2001
For	:	PREVENTING ID SPOOFING WITH UBIQUITOUS SIGNATURE CERTIFICATES
Group Art Unit	:	2137
Examiner	:	Kevin R. Schubert
Attorney Docket No.	:	NG(MS)7185

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Pursuant to the Notice of Non-Compliant Appeal Brief issued on August 28, 2006, Appellant presents herewith this Appeal Brief.

I. TABLE OF CONTENTS

II. REAL PARTY IN INTEREST

The real party in interest is Northrop Grumman Corporation, as indicated by the Assignment recorded August 11, 2004, Reel/Frame: 013751/0849.

III. RELATED APPEAL AND INTERFERENCES

There are no related appeals or interferences.

IV. STATUS OF CLAIMS

Claims 1-16, which are attached in the first Appendix, are currently pending in this application. Claims 1-2 and 9-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,878,138 to Yacobi ("Yacobi") in view of the following URL: http://web.archive.org/web/20000303141313/www.txdps.state.tx.us/administration/driver_licensing_control/faq.htm, for the Texas Department of Public Safety ("Texas DPS"). Claims 5-6 and 13-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yacobi in view of U.S. Patent No. 6,308,277 to Vaeth ("Vaeth"). Claims 3 and 11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yacobi in view of Texas DPS in further view of Zhou, Tao "Directory Integration and the Metadirectory", July 1999, Windows IT Pro ("Zhou"). Claims 7 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yacobi in view of

Vaeth in further view of Zhou. Claims 4 and 12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yacobi in view of Texas DPS in further view of U.S. Patent No. 5,214,702 to Fischer ("Fischer"). Claims 8 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yacobi in view of Vaeth in further view of Fischer.

The rejection of claims 1-16 is appealed.

V. STATUS OF AMENDMENTS

A response to a Final Office Action (hereinafter, "Final Rejection") issued on February 15, 2006 was filed on March 29, 2006. No amendments of the claims were filed after the Final Rejection. An Advisory Action Before Filing an Appeal Brief (hereinafter, "Advisory Action") dated April 10, 2006 was issued. The Advisory Action indicated that the request for reconsideration set forth in the Response to the Final Rejection was considered, but did not place the application in condition for allowance. At the time that Applicant's representative filed the notice of Appeal, Applicant's representative also requested a pre-appeal review of the application. The pre-appeal review was conducted, but did not place the application in condition for allowance.

VI. SUMMARY OF THE CLAIMED SUBJECT MATTER

A. Claim 1

One aspect of the present invention, as recited in claim 1 is directed to a method (Para. [0013]) of preventing ID spoofing of a public key infrastructure system in an enterprise (100 of FIG. 1) comprising allowing a user (132 of FIG. 3) to access a registration server (124 of FIG. 3) (Para. [0031]). The method also comprises that upon the registration server (124 of FIG. 3) receiving identification information from the user (132 of FIG. 3) and also receiving a request by the user (132 of FIG. 3) for a new signature certificate, the registration server (124 of FIG. 3) querying a directory (108 of FIG. 3) containing reference information of users of the enterprise (100 of FIG. 1) to obtain information regarding the identified user (132 of FIG. 3) (Para. [0031]). The method further comprises upon the registration server (124 of FIG. 3) receiving information from the directory (108 of FIG. 3) indicating that the identified user already possesses a signature certificate, the registration server (124 of FIG. 3) informing the user (132 of FIG. 3) that a new signature certificate will not be issued until the old signature certificate has been revoked (Para. [0031]), thereby preventing an unauthorized user (236 of FIG. 3) from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise (100 of FIG. 1) and signature certificates (Para. [0028]).

B. Claim 5

Another aspect of the present invention, as recited claim 5 is directed to a method (Para. [0014]) of preventing ID spoofing of a public key infrastructure system in an enterprise (100 of FIG. 1) comprising allowing a user (132 of FIG. 3) to access a registration server (124 of FIG. 3) (Para. [0034]). The method also comprises that upon the registration server (124 of FIG. 3) receiving identification information from the user (132 of FIG. 3) and also receiving a request by the user (132 of FIG. 3) for a new signature certificate, the registration server (124 of FIG. 3) querying a directory (108 of FIG. 3) containing reference information of users of the enterprise (100 of FIG. 1) to obtain information regarding the identified user (Para. [0034]). The method further comprises that upon the registration server (124 of FIG. 3) receiving information from the directory (108 of FIG.3) indicating that the identified user is not in the directory, the registration server (124 of FIG. 3) informing the user that a signature certificate will not be issued (Para. [0034]), thereby preventing an unauthorized user (236 of FIG. 3) from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise (100 of FIG. 1) and signature certificates (Para. [0028]).

C. Claim 9

Yet another aspect of the present invention, as recited in claim 9 is directed to an apparatus (Para. [0013]) for preventing ID spoofing of a public key

infrastructure system in an enterprise (100 of FIG. 1) comprising a registration server (124 of FIG. 3) to allow access by a user (Para. [0031]). The apparatus also comprises a directory (108 of FIG. 3) accessible by the registration server (124 of FIG. 3), the directory (108 of FIG. 3) storing information regarding all users in the enterprise (Para. [0021]). The apparatus also comprises that upon the registration server (124 of FIG. 3) receiving identification information from the user (132 of FIG. 3) and also receiving a request by the user (132 of FIG. 3) for a new signature certificate, the registration server (124 of FIG. 3) querying the directory (108 of FIG. 3) to obtain information regarding the identified user (Para. [0031]). The method further comprises upon the registration server (124 of FIG. 3) receiving information from the directory (108 of FIG. 3) indicating that the identified user already possesses a signature certificate, the registration server (124 of FIG.3) informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked (Para. [0031]), thereby preventing an unauthorized user (236 of FIG. 3) from ID spoofing to obtain a valid signature certificate such that the directory maintains a one-to-one correspondence between users of the enterprise (100 of FIG. 1) and signature certificates (Para. [0028]).

D. Claim 13

Yet a further aspect of the present invention, as recited in claim 13 is directed to an apparatus for preventing ID spoofing of a public key infrastructure

system in an enterprise (100 of FIG. 1) comprising a registration server (124 of FIG. 3) that allows to access by a user (132 of FIG.3) (Para. [0034]). The apparatus also comprises a directory (108 of FIG.3) storing information regarding all users in the enterprise (100 of FIG. 1) (Para. [0021]). The apparatus further comprises that upon the registration server (100 of FIG. 1) receiving identification information from the user (132 of FIG. 3) and also receiving a request by the user (132 of FIG. 3) for a new signature certificate, the registration server (124 of FIG. 3) querying the directory (108 of FIG. 3) to obtain information regarding the identified user (Para. [0034]). The apparatus still further comprises that upon the registration server (124 of FIG. 3) receiving information from the directory (108 of FIG. 3) indicating that the identified user is not in the directory (108 of FIG. 3), the registration server (124 of FIG. 3) informing the user (132 of FIG. 3) that the user (132 of FIG. 3) is not a valid member of the enterprise and not issue a signature certificate (Para. [0034]), such that the directory (108 of FIG. 3) maintains a one-to-one correspondence between users of the enterprise (100 of FIG. 1) and signature certificates (Para. [0028]).

VII. GROUNDS OF REJECTION TO BE REVIEW ON APPEAL

A. Whether claims 1-2 and 9-10 are made obvious under 35 U.S.C. §103(a) by Yacobi in view of Texas DPS?

B. Whether claim 5-6 and 13-14 are made obvious under 35 U.S.C. §103(a) by Yacobi in view of Vaeth?

C. Whether claims 3 and 11 are made obvious under 35 U.S.C. §103(a) by Yacobi in view of Texas DPS and in further view of Zhou?

D. Whether claims 7 and 15 are made obvious under 35 U.S.C. §103(a) by Yacobi in view of Vaeth and in further view of Zhou?

E. Whether claims 4 and 12 are made obvious under 35 U.S.C. §103(a) by Yacobi in view of Texas DPS and in further view of Fischer?

F. Whether claims 8 and 16 are made obvious under 35 U.S.C. §103(a) by Yacobi in view of Vaeth and in further view of Fischer?

VIII. ARGUMENTS FOR CLAIMS

A. 35 U.S.C. §103(a) rejection of claims 1-2 and 9-10 as being made obvious by Yacobi in view of Texas DPS

The Court of Customs and Patent Appeals has held that to establish prima facie obviousness of a claimed invention, all the claimed limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974).

1. The Obviousness Rejection of claim 1

Claim 1 is patentable over Yacobi in view of Texas DPS for at least the following reasons:

a. Neither Yacobi nor Texas DPS teaches or suggests a method

of preventing ID spoofing of a public key infrastructure system in an enterprise that includes allowing a user to access a registration server, and upon the registration server receiving information from a directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates, as recited in claim 1.

Claim 1 recites a method of preventing ID spoofing of a public key infrastructure system in an enterprise comprising allowing a user to access a registration server. Claim 1 also recites that upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user. Claim 1 further recites that upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user

from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

In the Final Rejection, the Examiner admits that Yacobi does not teach or suggest informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked, as recited in claim 1. However, the Examiner contends that Texas DPS makes up for the deficiencies of Yacobi, with respect to claim 1. Applicant's representative respectfully disagrees with this contention. Texas DPS discloses that in order for a person to get a Texas driver's license, that person will be required to surrender his/her valid or expired Out-of-State driver's license (See Texas DPS, Page 1). A driver's license (from any State) is not a signature certificate. A signature certificate is a form of a digital certificate. A digital certificate contains information identifying the owner of a key pair, a public key of the key pair, and a period for which the certificate is valid (See Spec., Para. [0004]). There is no teaching or suggestion in Texas DPS that a driver's license contains a public key of a key pair, like the signature certificate recited in claim 1. In fact, Texas DPS is devoid of any process or structure that could be construed as a signature certificate, as recited in claim 1. Thus, Texas DPS does not teach or suggest informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked, as recited in claim 1. Accordingly, Yacobi and Texas DPS, taken individually or in combination do not teach or suggest each and every element of

claim 1.

b. There is no motivation to combine and modify the teachings of Yacobi and Texas DPS in the manner suggested by the Examiner.

The United States Court of Appeals for the Federal Circuit ("Federal Circuit") has held that obviousness cannot be established by combining teachings of multiple references to produce a claimed invention, absent some teaching or suggestion supporting the combination. *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1574, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984).

Yacobi discloses electronic wallets that are tamper-resistant and portable (See Yacobi, Col. 5, Lines 17-19). In Yacobi, when an electronic wallet is renewing a certificate the electronic wallet submits the old certificate before a new one is issued (See Yacobi, Col. 12, Lines 18-22). The process is automatic, and Yacobi does not teach or suggest any user interaction during the certificate renewal process. In rejecting claim 1, the Examiner contends in the Final Rejection that it would be obvious to combine the ideas of Texas DPS with those of Yacobi to "inform" a user of a surrender so that the user is better aware of the process taking place (See Final Rejection, Page 3, Lines 16-18). However, Applicant's representative respectfully submits that the reason given by the Examiner for the motivation to combine the references would change the principle of operation of Yacobi.

The Court of Customs and Patent Appeals has held that if a proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti,* 270 F.2d 810, 813, 12 U.S.P.Q. 349 (C.C.P.A. 1959). Yacobi discloses some typical uses for the electronic wallets, including employing the electronic wallets at an automatic teller machine (ATM), and for purchasing tokens on a public transportation system (See Yacobi, Col. 5, Lines 28-43). Clearly, the electronic wallets disclosed in Yacobi are designed to be employed by laypersons. Including informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked, as recited in claim 1, would add unneeded and unwanted complexity to the renewal process disclosed in Yacobi. In Yacobi, there is nothing to indicate that users of the electronic wallets are even aware of the existence of the certificates in the electronic wallets. Thus, combining and modifying the teachings of Yacobi and Texas DPS in the manner suggested by the Final Rejection would change the principle of operation of Yacobi. Accordingly, absent the present application, there is no motivation to combine and modify the teachings of Yacobi and Texas DPS.

c. Texas DPS is non-analogous art with respect to claim 1.

The Federal Circuit has held that in order for cited art to be analogous, and maintain a prima facie case of obviousness, the cited art must be in the

same field of endeavor or be reasonably pertinent to the problem the inventor is attempting to solve. *Wang Lab., Inc. v. Toshiba Corp.*, 993 F.2d 858, 863 26 U.S.P.Q.2d 1767, 1773 (Fed. Cir. 1993). Applicant's representative submits that Texas DPS is non-analogous art with respect to claim 1 for at least the following reasons.

Applicant's representative respectfully submits that Texas DPS is not in the same field of endeavor as claim 1. In the Final Rejection, the Examiner admits that Texas DPS and the present application's specification relate to different forms of identification (See Final Rejection, Page 8). In *Wang*, the Federal Circuit considered patent claims which were directed to single inline memory modules (SIMMs) for installation on a printed circuit motherboard for use in personal computers. 993 F.2d 858, 861, 26 U.S.P.Q.2d 1767. In *Wang*, the Federal Circuit held that a second patent that discloses a SIMM containing nine memory chips, eight for storing data and one for error detection, mounted in a single row was not in the same field of endeavor as the claimed invention. 993 F.2d 858, 864, 25 U.S.P.Q2d 1767. Moreover, in *Wang* the Federal Circuit concluded that the two patents were not in the same field of endeavor merely because they related to memories. 993 F.2d 858, 864, 26 U.S.P.Q.2d 1767. It is respectfully submitted that the *Wang* case considered art fields that were closer than claim 1 and Texas DPS.

Claim 1 is directed to public key infrastructures (PKIs), while Texas DPS is directed to administration of driver's licenses. A person can identify the holder of a driver's license by looking at the picture on the driver's license and comparing the picture to the person presenting the license. On the other hand, a computer can only identify the presenter of a signature certificate by executing a computer algorithm. Unlike a driver's license, a person cannot identify the presenter of a signature certificate without the assistance of a computer. Thus, Applicant's representative respectfully submits that claim 1 and Texas DPS are not in the same field of endeavor because they relate to different forms of identification.

Additionally, Applicant's representative respectfully submits that Texas DPS is not reasonably pertinent to the problem being solved by claim 1. In *In re Clay* the Federal Circuit set forth a test to determine if a reference is reasonably pertinent to a problem being solved by a claimed invention. 966 F.2d 658, 23 U.S.P.Q.2d 1058, 1060-1061 (Fed. Cir. 1992). In *In re Clay*, the Federal Circuit held that a reference is reasonably pertinent if the reference, because of the matter with which it deals, logically would have commended itself to the attention in considering his problem. 966 F.2d 658, 23 U.S.P.2d 1058, 1061. In *In re Clay*, the Federal Circuit held that a reference which disclosed gel treatment of underground formation functions to fill anomalies was not reasonably pertinent to a gel function to displace liquid from dead volume of a storage tank. 966 F.2d 658, 23 U.S.P.Q.2d 1058, 1061. It is respectfully submitted that the present case

is analogous to *In re Clay*, in that one skilled in the art of PKI certificates (claim 1) would not look to a driver's license administration procedure (Texas DPS) to implement the subject matter of claim 1.

In the Advisory Action, the Examiner contends that Texas DPS is reasonably pertinent because it addresses identity spoofing (See Advisory Action, Page 2). Applicant's representative respectfully disagrees with this contention. The process disclosed in Texas DPS is related to a relatively insecure administration of driver's licenses. In fact, Texas DPS discloses that if a person loses his/her driver's license, that person can still obtain a new one (See Texas DPS, page 1). Claim 1 relates to administration of signature certificates in a high security PKI. The vast differences in the security levels of the method of claim 1 and Texas DPS would not lead one skilled in the art of PKI administration to find that the process disclosed by Texas DPS was reasonably pertinent to the problem being solved by claim 1. Thus, Texas DPS would not have commended itself to one skilled in the art since Texas DPS operates in a completely different fashion than claim 1. Accordingly, Texas DPS is not reasonably pertinent to the problem being solved by claim 1, and Applicant's representative respectfully submits that Texas DPS is non-analogous art with respect to claim 1.

For the reasons stated above, Yacobi taken in view of Texas DPS does not make claim 1 obvious. Therefore, claim 1 should be patentable over the

cited art. Thus, Applicant's representative respectfully requests that the rejection of claim 1 be withdrawn.

2. **The Obviousness Rejection of Claim 2**

Claim 2 depends from claim 1 and is patentable over Yacobi in view of Texas DPS for at least the same reasons as claim 1, and for the specific elements recited therein. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 2.

3. **The Obviousness Rejection of Claim 9**

Claim 9 is patentable over Yacobi in view of Texas DPS for at least the following reasons:

a. **Neither Yacobi nor Texas DPS teaches or suggests an apparatus for preventing ID spoofing of a public key infrastructure system in an enterprises that includes a registration server to allow access by a user and upon the registration server receiving information from a directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate, such that the directory maintains a one-**

to-one correspondence between users of the enterprise and signature certificates, as recited in claim 9.

Claim 9 recites an apparatus for preventing ID spoofing of a public key infrastructure system in an enterprise comprising a registration server to allow access by a user. Claim 9 additionally recites a directory accessible by the registration server, the directory storing information regarding all users in the enterprise. Claim 9 also recite that upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user. Claim 9 further recites that upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate such that the directory maintains a one-to-one correspondence between users of the enterprise and signature certificates.

In the Final Rejection, the Examiner admits that Yacobi does not teach or suggest informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked, as recited in claim 9. However, the Examiner contends that Texas DPS makes up for the deficiencies of Yacobi,

with respect to claim 9. Applicant's representative respectfully disagrees with this contention. Texas DPS discloses that in order for a person to get a Texas driver's license, that person will be required to surrender his/her valid or expired Out-of-State driver's license (See Texas DPS, Page 1). A driver's license (from any State) is not a signature certificate. A signature certificate is a form of a digital certificate. A digital certificate contains information identifying the owner of a key pair, a public key of the key pair, and a period for which the certificate is valid (See Spec., Para. [0004]). There is no teaching or suggestion in Texas DPS that a driver's license contains a public key of a key pair, like the signature certificate recited in claim 9. In fact, Texas DPS is devoid of any process or structure that could be construed as a signature certificate, as recited in claim 9. Thus, Texas DPS does not teach or suggest a registration server informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked, as recited in claim 9. Accordingly, Yacobi and Texas DPS, taken individually or in combination do not teach or suggest each and every element of claim 9.

b. There is no motivation to combine and modify the teachings of Yacobi and Texas DPS in the manner suggested by the Examiner.

The United States Court of Appeals for the Federal Circuit ("Federal Circuit") has held that obviousness cannot be established by combining teachings of multiple references to produce a claimed invention, absent some

teaching or suggestion supporting the combination. *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1574, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984).

Yacobi discloses electronic wallets that are tamper-resistant and portable (See Yacobi, Col. 5, Lines 17-19). In Yacobi, when an electronic wallet is renewing a certificate the electronic wallet submits the old certificate before a new one is issued (See Yacobi, Col. 12, Lines 18-22). The process is automatic, and Yacobi does not teach or suggest any user interaction during the certificate renewal process. In rejecting claim 9, the Examiner contends in the Final Rejection that it would be obvious to combine the ideas of Texas DPS with those of Yacobi to "inform" a user of a surrender so that the user is better aware of the process taking place (See Final Rejection, Page 3, Lines 16-18). However, Applicant's representative respectfully submits that the reason given by the Examiner for the motivation to combine the references would change the principle of operation of Yacobi.

The Court of Customs and Patent Appeals has held that if a proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti,* 270 F.2d 810, 813, 12 U.S.P.Q. 349 (C.C.P.A. 1959). Yacobi discloses some typical uses for the electronic wallets, including employing the electronic wallets at an automatic teller machine (ATM), and for purchasing tokens on a public

transportation system (See Yacobi, Col. 5, Lines 28-43). Clearly, the electronic wallets disclosed in Yacobi are designed to be employed by laypersons. Including a registration server informing a user that a new signature certificate will not be issued until the old signature certificate has been revoked, as recited in claim 9, would add unneeded and unwanted complexity to the renewal process disclosed in Yacobi. In Yacobi, there is nothing to indicate that users of the electronic wallets are even aware of the existence of the certificates in the electronic wallets. Thus, combining and modifying the teachings of Yacobi and Texas DPS in the manner suggested by the Final Rejection would change the principle of operation of Yacobi. Accordingly, absent the present application, there is no motivation to combine and modify the teachings of Yacobi and Texas DPS.

c. Texas DPS is non-analogous art with respect to the apparatus recited in claim 9.

The Federal Circuit has held that in order for cited art to be analogous, and maintain a prima facie case of obviousness, the cited art must be in the same field of endeavor or be reasonably pertinent to the problem the inventor is attempting to solve. *Wang Lab., Inc. v. Toshiba Corp.*, 993 F.2d 858, 863 26 U.S.P.Q.2d 1767, 1773 (Fed. Cir. 1993). Applicant's representative submits that Texas DPS is non-analogous art with respect to claim 9 for at least the following reasons.

Applicant's representative respectfully submits that Texas DPS is not in the same field of endeavor as the apparatus recited in claim 9. In the Final Rejection, the Examiner admits that Texas DPS and the present application's specification relate to different forms of identification (See Final Rejection, Page 8). In *Wang*, the Federal Circuit considered patent claims which were directed to single inline memory modules (SIMMs) for installation on a printed circuit motherboard for use in personal computers. 993 F.2d 858, 861, 26 U.S.P.Q.2d 1767. In *Wang*, the Federal Circuit held that a second patent that discloses a SIMM containing nine memory chips, eight for storing data and one for error detection, mounted in a single row was not in the same field of endeavor as the claimed invention. 993 F.2d 858, 864, 25 U.S.P.Q2d 1767. Moreover, in *Wang* the Federal Circuit concluded that the two patents were not in the same field of endeavor merely because they related to memories. 993 F.2d 858, 864, 26 U.S.P.Q.2d 1767. It is respectfully submitted that the *Wang* case considered art fields that were closer than the apparatus recited in claim 9 and Texas DPS.

Claim 9 is directed to public key infrastructures (PKIs), while Texas DPS is directed to administration of driver's licenses. A person can identify the holder of a driver's license by looking at the picture on the driver's license and comparing the picture to the person presenting the license. On the other hand, a computer can only identify the presenter of a signature certificate by executing a computer algorithm. Unlike a driver's license, a person cannot identify the presenter of a

signature certificate without the assistance of a computer. Thus, Applicant's representative respectfully submits that the apparatus recited in claim 9 and Texas DPS are not in the same field of endeavor because they relate to different forms of identification.

Additionally, Applicant's representative respectfully submits that Texas DPS is not reasonably pertinent to the problem being solved by the apparatus recited in claim 9. In *In re Clay* the Federal Circuit set forth a test to determine if a reference is reasonably pertinent to a problem being solved by a claimed invention. 966 F.2d 658, 23 U.S.P.Q.2d 1058, 1060-1061 (Fed. Cir. 1992). In *In re Clay*, the Federal Circuit held that a reference is reasonably pertinent if the reference, because of the matter with which it deals, logically would have commended itself to the attention in considering his problem. 966 F.2d 658, 23 U.S.P.2d 1058, 1061. In *In re Clay*, the Federal Circuit held that a reference which disclosed gel treatment of underground formation functions to fill anomalies was not reasonably pertinent to a gel function to displace liquid from dead volume of a storage tank. 966 F.2d 658, 23 U.S.P.Q.2d 1058, 1061. It is respectfully submitted that the present case is analogous to *In re Clay*, in that one skilled in the art of PKI certificates (claim 9) would not look a driver's license administration procedure (Texas DPS) to implement the subject matter of claim 9.

In the Advisory Action, the Examiner contends that Texas DPS is reasonably pertinent because it addresses identity spoofing (See Advisory Action, Page 2). Applicant's representative respectfully disagrees with this contention. The process disclosed in Texas DPS is related to a relatively insecure administration of driver's licenses. In fact, Texas DPS discloses that if a person loses his/her driver's license, that person can still obtain a new one (See Texas DPS, page 1). Claim 9 relates to an apparatus for administration of signature certificates in a high security PKI. The vast differences in the security levels of the apparatus of claim 9 and Texas DPS would not lead one skilled in the art of PKI administration to find that the process disclosed by Texas DPS was reasonably pertinent to the problem being solved by claim 9. Thus, Texas DPS would not have commended itself to one skilled in the art since Texas DPS operates in a completely different fashion than claim 9. Accordingly, Texas DPS is not reasonably pertinent to the problem being solved by claim 9, and Applicant's representative respectfully submits that Texas DPS is non-analogous art with respect to the apparatus recited in claim 9.

For the reasons stated above, Yacobi taken in view of Texas DPS does not make the apparatus recited in claim 9 obvious. Therefore, claim 9 should be patentable over the cited art. Thus, Applicant's representative respectfully requests that the rejection of claim 9 be withdrawn.

4. The Obviousness Rejection of Claim 10

Claim 10 depends from claim 9 and is patentable over Yacobi in view of Texas DPS for at least the same reasons as claim 9, and for the specific elements recited therein. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 10.

B. 35 U.S.C. §103(a) rejection of claims 5-6 and 13-14 as being made obvious by Yacobi in view of Texas DPS

The Court of Customs and Patent Appeals has held that to establish prima facie obviousness of a claimed invention, all the claimed limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974).

1. The Obviousness Rejection of claim 5

Claim 5 is patentable over Yacobi in view of Vaeth for at least the following reasons:

a. Neither Yacobi nor Vaeth teach or suggest a method for preventing ID spoofing in a public key infrastructure in an enterprise that includes allowing a user to access a registration server, as recited in claim 5, when claim 5 is read as a whole.

Claim 5 recites a method of preventing ID spoofing of a public key infrastructure system in an enterprise comprising allowing a user to access a

registration server. Claim 5 also recites that upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user. Claim 5 further recites that upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

When claim 5 is read as whole, it is clear that the user recited in claim 5 does not possess a valid signature certificate. Applicant's representative respectfully submits that in rejecting claim 5, the Examiner does not read claim 5 "as a whole." The Federal Circuit has held that to support a determination of obviousness, the actual determination of the issue requires an evaluation in light of the findings in those inquiries of the obviousness of the claimed invention *as a whole*, not merely the differences between the claimed invention and the prior art. *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, U.S.P.Q. 1024, 1033 (Fed. Cir. 1984). When read as a whole, it is clear that the user recited in claim 5 is requesting a new signature certificate. The user would not request a new

signature certificate if the user already possessed a signature certificate. Additionally, if the user were to possess a signature certificate, the user would be in the directory recited in claim 5, since the directory contains reference information of users of an enterprise. Thus, it is clear that when claim 5 is read as a whole, the user recited in claim 5 does not possess a signature certificate.

In the Final Rejection, the Examiner contends that Yacobi taken in view of Vaeth renders claim 5 obvious (See Final Rejection, Page 4). In rejecting claim 5, the Examiner contends that Yacobi discloses allowing a user to access a registration server (See Final Rejection, Page 4). However, the referenced section of Yacobi discloses a user possessing an electronic wallet with a manufacturer-issued certificate, wherein the user is re-certified, and issued another certificate (See Yacobi, Col. 8, Line 40-Col. 9, Line 23). Yacobi presupposes that any user attempting to have a certificate issued is in possession of an electronic wallet, and therefore, the user is already in possession of a certificate. In Yacobi, the electronic wallet (that already possess a certificate) acts as a key that allows a user to access a certification authority. Without physical possession of the electronic wallet (and therefore, possession of a certificate) the user cannot request a new certificate. Thus, Yacobi does not teach or suggest allowing a user to access a registration server, as recited in claim 5, when claim 5 is read as a whole.

b. Neither Yacobi nor Vaeth teach or suggest that upon a registration server receiving identification from a user and also receiving a request by the user for a new certificate, the registration server querying a directory containing reference information of users of an enterprise to obtain information regarding the identified user, as recited in claim 5.

For the reasons stated above, when read as a whole the user recited in claim 5 does not possess a certificate. In contrast, Yacobi discloses that any user requesting a certificate already possesses a certificate. In Yacobi, a bank computer confirms the identity of a user if an electronic wallet's certificate checks out cleanly (See Yacobi, Col. 9, Lines 15-20). Thus, Yacobi does not teach or suggest a registration server receiving identification information from a user and also receiving a request by the user for a new signature certificate, as recited in claim 5.

c. There is no motivation to combine and modify the teachings of Yacobi in view of Vaeth in the manner suggested by the Final Rejection.

Applicant's representative respectfully submits that there is no motivation to combine and modify the teachings of Yacobi and Vaeth in the manner suggested by the Examiner in the Final Rejection. As admitted in the Final rejection, Yacobi fails to teach or suggest that upon a registration server indicating that an identified user is not in a directory, the registration server informing the user that a signature certificate will not be issued, as recited in

claim 5 (See Final Rejection, Page 4). The Examiner contends that Vaeth cures the deficiencies of Yacobi. Applicant's representative respectfully disagrees with the Examiner's contention. Applicant's representative respectfully submits that in Yacobi, any user requesting a certificate is already in possession of a certificate. It would not have been obvious to one of ordinary skill in the art implementing Yacobi to include the step of upon a registration server receiving information from a directory indicating that an identified user in not in a directory, the registration server informing the user that a signature certificate will not be issued, as recited in claim 5.

Moreover, in the Final Rejection, the Examiner contends that the combination of Yacobi and Vaeth would not result in a less secure system (See Final Rejection, Page 9). Applicant's representative respectfully disagrees. Vaeth discloses that a requestor using an Internet browser can request certificate using a certificate request web page (See Vaeth, Col. 7, Lines 55-61). Thus, in Vaeth, any person with an Internet browser can request a certificate. There is no requirement in Vaeth that the requestor posses any special piece of hardware (i.e., an electronic wallet with a certificate, as disclosed in Yacobi). Thus, combining the teachings of Vaeth with the teachings of Yacobi would cause the system of Yacobi to be less secure. The combined system would be less secure because signature certificates and private keys can be easily copied off personal computers that include Internet browsers (e.g., by computer viruses, hackers,

etc.). In contrast, in Yacobi, physical possession of the electronic wallet acts as a key. The electronic wallets disclosed in Yacobi are tamper resistant (See Yacobi, Col. 5, Lines 17-18). Thus, the certificate and/or private key on an electronic wallet disclosed in Yacobi could not be easily copied. The Federal Circuit has held that motivation to combine concerns what is desirable, not just what is feasible. *Winner Intl. Royalty Corp. v. Ching-Rong Wang* 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1587 (Fed. Cir. 2000). In *Winner Intl. Royalty Corp*, the Federal Circuit held that one of ordinary skill in the art would not have reasonably elected trading the benefit of security for that of convenience. 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1587.

Applicant's representative respectfully submits that one of ordinary skill in the art would not trade the benefit of security offered by Yacobi, by requiring a user requesting a new certificate to possess an electronic wallet, for the convenience offered by Vaeth by allowing anyone with an Internet browser to request a new certificate. Accordingly, Applicant's representative respectfully submits that there is no motivation to combine and modify the teachings of Yacobi and Vaeth in the Manner suggested by the Examiner.

For the reasons stated above, Yacobi in view of Vaeth does not make claim 5 obvious. Therefore, claim 5 should be patentable over the cited art. Thus, Applicant's representative respectfully requests that the rejection of claim 5 be withdrawn.

2. **The Obviousness Rejection of Claim 6**

Claim 6 depends from claim 5 and is patentable over Yacobi in view of Vaeth for at least the same reasons as claim 5, and for the specific elements recited therein. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 6.

3. **The Obviousness Rejection of Claim 13**

Claim 13 is patentable over Yacobi in view of Vaeth for at least the following reasons:

a. Neither Yacobi nor Vaeth teach or suggest an apparatus for preventing ID spoofing of a public key infrastructure in an enterprise that includes a registration server to allow access by a user, as recited in claim 13, when claim 13 is read as a whole.

Claim 13 recites an apparatus for preventing ID spoofing of a public key infrastructure system in an enterprise comprising a registration server to allow to access by a user. Claim 13 also recites a directory storing information regarding all users in the enterprise. Claim 13 further recites that upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user. Claim

13 still further recites that upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that the user is not a valid member of the enterprise and not issue a signature certificate, such that the directory maintains a one-to-one correspondence between users of the enterprise and signature certificates.

When claim 13 is read as whole, it is clear that the user recited in claim 13 does not possess a valid signature certificate. Applicant's representative respectfully submits that in rejecting claim 13, the Examiner does not read claim 13 "as a whole." The Federal Circuit has held that to support a determination of obviousness, the actual determination of the issue requires an evaluation in light of the findings in those inquiries of the obviousness of the claimed invention *as a whole*, not merely the differences between the claimed invention and the prior art. *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, U.S.P.Q. 1024, 1033 (Fed. Cir. 1984). When read as a whole, it is clear that the user recited in claim 13 is requesting a new signature certificate. The user would not request a new signature certificate if the user already possessed a signature certificate. Additionally, if the user were to possess a signature certificate, the user would be in the directory recited in claim 13, since the directory stores information regarding all users of an enterprise. Thus, it is clear that when claim 13 is read as a whole, the user recited in claim 13 does <u>not</u> possess a signature certificate.

In the Final Rejection, the Examiner contends that Yacobi taken in view of Vaeth renders claim 13 obvious (See Final Rejection, Page 4). In rejecting claim 13, the Examiner contends that Yacobi discloses a registration server to allow access by a user (See Final Rejection, Page 4). However, the referenced section of Yacobi discloses a user possessing an electronic wallet with a manufacturer-issued certificate, wherein the user is re-certified, and issued another certificate (See Yacobi, Col. 8, Line 40-Col. 9, Line 23). Yacobi presupposes that any user attempting to have a certificate issued is in possession of an electronic wallet, and therefore, the user is already in possession of a certificate. In Yacobi, the electronic wallet (that already possess a certificate) acts as a key that allows a user to access a certification authority. Without physical possession of the electronic wallet (and therefore, possession of a certificate) the user cannot request a new certificate. Thus, Yacobi does not teach or suggest a registration server to allow access by a user, as recited in claim 13, when claim 13 is read as a whole.

b. Neither Yacobi nor Vaeth teach or suggest that upon a registration server receiving identification from a user and also receiving a request by the user for a new certificate, the registration server querying a directory to obtain information regarding the identified user, as recited in claim 13.

For the reasons stated above, when read as a whole the user recited in claim 13 does not possess a certificate. In contrast, Yacobi discloses that any user requesting a certificate already possesses a certificate. In Yacobi, a bank computer confirms the identity of a user if an electronic wallet's certificate checks out cleanly (See Yacobi, Col. 9, Lines 15-20). Thus, Yacobi does not teach or suggest a registration server receiving identification information from a user and also receiving a request by the user for a new signature certificate, as recited in claim 13.

c. There is no motivation to combine and modify the teachings of Yacobi in view of Vaeth in the manner suggested by the Final Rejection.

Applicant's representative respectfully submits that there is no motivation to combine and modify the teachings of Yacobi and Vaeth in the manner suggested by the Examiner in the Final Rejection. As admitted in the Final rejection, Yacobi fails to teach or suggest that upon a registration server indicating that an identified user is not in a directory, the registration server informing the user that a signature certificate will not be issued, as recited in

claim 13 (See Final Rejection, Page 4). The Examiner contends that Vaeth cures the deficiencies of Yacobi. Applicant's representative respectfully disagrees with the Examiner's contention. Applicant's representative respectfully submits that in Yacobi, any user requesting a certificate is already in possession of a certificate. It would not have been obvious to one of ordinary skill in the art implementing Yacobi to include the step of upon a registration server receiving information from a directory indicating that an identified user in not in a directory, the registration server informing the user that a signature certificate will not be issued, as recited in claim 13.

Moreover, in the Final Rejection, the Examiner contends that the combination of Yacobi and Vaeth would not result in a less secure system (See Final Rejection, Page 9). Applicant's representative respectfully disagrees. Vaeth discloses that a requestor using an Internet browser can request certificate using a certificate request web page (See Vaeth, Col. 7, Lines 55-61). Thus, in Vaeth, any person with an Internet browser can request a certificate. There is no requirement in Vaeth that the requestor posses any special piece of hardware (i.e., an electronic wallet with a certificate, as disclosed in Yacobi). Thus, combining the teachings of Vaeth with the teachings of Yacobi would cause the system of Yacobi to be less secure. The combined system would be less secure because signature certificates and private keys can be easily copied off personal computers that include Internet browsers (e.g., by computer viruses, hackers,

etc.). In contrast, in Yacobi, physical possession of the electronic wallet acts as a key. The electronic wallets disclosed in Yacobi are tamper resistant (See Yacobi, Col. 5, Lines 17-18). Thus, the certificate and/or private key on an electronic wallet disclosed in Yacobi could not be easily copied. The Federal Circuit has held that motivation to combine concerns what is desirable, not just what is feasible. *Winner Intl. Royalty Corp. v. Ching-Rong Wang* 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1587 (Fed. Cir. 2000). In *Winner Intl. Royalty Corp*, the Federal Circuit held that one of ordinary skill in the art would not have reasonably elected trading the benefit of security for that of convenience. 202 F.3d 1340, 1349, 53 U.S.P.Q.2d 1587.

Applicant's representative respectfully submits that one of ordinary skill in the art would not trade the benefit of security offered by Yacobi, by requiring a user requesting a new certificate to possess an electronic wallet, for the convenience offered by Vaeth by allowing anyone with an Internet browser to request a new certificate. Accordingly, Applicant's representative respectfully submits that there is no motivation to combine and modify the teachings of Yacobi and Vaeth in the Manner suggested by the Examiner.

For the reasons stated above, Yacobi in view of Vaeth does not make the apparatus recited in claim 13 obvious. Therefore, claim 13 should be patentable over the cited art. Thus, Applicant's representative respectfully requests that the rejection of claim 13 be withdrawn.

4. The Obviousness Rejection of Claim 14

Claim 14 depends from claim 13 and is patentable over Yacobi in view of Vaeth for at least the same reasons as claim 13, and for the specific elements recited therein. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 14.

C. 35 U.S.C. §103(a) rejection of claims 3 and 11 as being made obvious by Yacobi in view of Texas DPS and in further view of Zhou

1. The Obviousness Rejection of Claim 3

Claim 3 depends from claim 1. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Texas DPS with respect to claim 1, from which claim 3 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 3.

2. The Obviousness Rejection of Claim 11

Claim 11 depends from claims 10 and 9. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Texas DPS with respect to claims 9 and 10, from which claim 11 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 11.

D. 35 U.S.C. §103(a) rejection of claims 7 and 15 as being made obvious by Yacobi in view of Vaeth and in further view of Zhou

1. The Obviousness Rejection of Claim 7

Claim 7 depends from claim 5. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Vaeth with respect to claim 5, from which claim 7 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 7.

2. The Obviousness Rejection of Claim 15

Claim 15 depends from claim 13. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Vaeth with respect to claim 13, from which claim 15 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 15.

E. 35 U.S.C. §103(a) rejection of claims 4 and 12 as being made obvious by Yacobi in view of Vaeth and in further view of Zhou

1. The Obviousness Rejection of Claim 4

Claim 4 depends from claim 1. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Texas DPS with respect to claim 1, from which claim 4 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 4.

2. The Obviousness Rejection of Claim 12

Claim 12 depends from claim 9. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Texas DPS with respect to claim 9, from which claim 12 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 12.

F. 35 U.S.C. §103(a) rejection of claims 8 and 16 as being made obvious by Yacobi in view of Vaeth and in further view of Fischer

1. The Obviousness Rejection of Claim 8

Claim 8 depends from claim 5. The further addition of Fischer does not make up for the aforementioned deficiencies of Yacobi taken in view of Vaeth with respect to claim 5, from which claim 8 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 8.

2. The Obviousness Rejection of Claim 16

Claim 16 depends from claim 13. The further addition of Zhou does not make up for the aforementioned deficiencies of Yacobi taken in view of Vaeth with respect to claim 13, from which claim 16 depends. Accordingly, Applicant's representative respectfully requests withdrawal of the rejection of claim 16.

IX. APPENDICES

The first attached Appendix contains a copy of the claims on appeal.

The second and third Appendices have been included to comply with statutory requirements.

Please charge any deficiency or credit any overpayment in the fees for this Appeal Brief to Deposit Account No. 20-0090.

Respectfully submitted,

Christopher P. Harris
Reg. No. 43,660

TAROLLI, SUNDHEIM, COVELL
& TUMMINO, L.L.P.
1300 East Ninth Street, Suite 1700
Cleveland, Ohio 44114
(216) 621-2234
(216) 621-4072 (Facsimile)
Customer No.: 26294

Claims Appendix

Claim 1 A method of preventing ID spoofing of a public key infrastructure system in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

Claim 2 The method of claim 1, further comprising providing user identifiers and their corresponding digital signature certificates in said directory.

Claim 3 The method of claim 1, further comprising providing an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

Claim 4 The method of claim 1, further comprising providing a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize a user.

Claim 5 A method of preventing ID spoofing of a public key infrastructure in an enterprise comprising: allowing a user to access a registration server; upon the registration server receiving identification information from the user and also receiving a request by the user for a new signature certificate, the registration server querying a directory containing reference information of users of the enterprise to obtain information regarding the identified user; and upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that a signature certificate will not be issued, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate and maintaining a one-to-one correspondence between users of the enterprise and signature certificates.

Claim 6 The method of claim 5, further comprising providing user identifiers and their corresponding digital signature certificates in said directory.

Claim 7 The method of claim 5, further comprising providing an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

Claim 8 The method of claim 5, further comprising providing a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize the user.

Claim 9 An apparatus for preventing ID spoofing of a public key infrastructure system in an enterprise comprising: a registration server to allow access by a user; a directory accessible by the registration server, the directory storing information regarding all users in the enterprise; wherein, upon the registration server receiving information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user; and wherein, upon the registration server receiving information from the directory indicating that the identified user already possesses a signature certificate, the

registration server informing the user that a new signature certificate will not be issued until the old signature certificate has been revoked, thereby preventing an unauthorized user from ID spoofing to obtain a valid signature certificate, such that the directory maintains a one-to-one correspondence between the users of the enterprise and signature certificates.

Claim 10 The apparatus of claim 9, wherein the directory includes identifiers and their corresponding digital signature certificates.

Claim 11 The apparatus of claim 10, further comprising an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

Claim 12 The apparatus of claim 9, further comprising a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize a user.

Claim 13 An apparatus for preventing ID spoofing of a public key infrastructure in an enterprise comprising: a registration server to allow access by a user; a directory accessible by the registration server, the directory storing information regarding all users in the enterprise; wherein, upon the registration

server receiving information from the user and also receiving a request by the user for a new signature certificate, the registration server querying the directory to obtain information regarding the identified user; and wherein, upon the registration server receiving information from the directory indicating that the identified user is not in the directory, the registration server informing the user that the user is not a valid member of the enterprise and not issue a signature certificate, such that the directory maintains a one-to-one correspondence between the users of the enterprise and signature certificates.

Claim 14 The apparatus of claim 13, wherein the directory includes identifiers and their corresponding digital signature certificates.

Claim 15 The apparatus of claim 13, further comprising an authoritative database including user identifiers, wherein the directory is updated from the authoritative database.

Claim 16 The apparatus of claim 13, further comprising a personal revocation authority to revoke a user's previous signature certificate, the personal revocation authority being chosen so as to personally recognize the user.

Evidence Appendix

None

Related Proceedings Appendix

None